WE ARE YOUR DOL

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Инструкции по настройке многофакторной аутентификации

Штат Нью-Йорк начал использовать многофакторную аутентификацию (MFA) в некоторых своих общественных приложениях.

MFA – это способ обеспечения защиты и безопасности вашей учетной записи. Этот способ защиты требует второго фактора для гарантии того, что вы тот, за кого себя выдаете, помимо простого пароля. Если вы используете приложение, защищенное MFA, даже если кто-то угадает или украдет ваш пароль, он все равно не сможет войти в систему без второго фактора. Если пароль – это то, что вы знаете, то второй фактор – это то, кем вы являетесь (обычно считывается биометрическим устройством) или то, что у вас есть.

Данный документ предназначен для оказания помощи клиентам в настройке многофакторной аутентификации для их учетной записи на сайте NY.gov.

СОДЕРЖАНИЕ

Настройка аутентификатора Google для многофакторной аутентификации

Если вы еще не зарегистрированы в MFA, вам будет предложено зарегистрироваться после входа в систему Labor Online Services и нажатия на кнопку подачи заявления «Unemployment Services».

На экране вашего компьютера появится окно с предложением настроить многофакторную аутентификацию.

- Загрузите на свой смартфон приложение Google Authenticator. Инструкции по скачиванию приложения см. ниже.
- На экране компьютера нажмите кнопку **Setup** в разделе Google Authenticator, чтобы начать процесс установки.
- Выберите iPhone или Android в зависимости от вашего устройства.
    - Вам будет предложено загрузить приложение Google Authenticator из Google Play Store (Android) или App Store (iPhone). Если вы еще не сделали этого, вам следует загрузить это приложение прямо сейчас. Инструкции по скачиванию приложения см. ниже.

  СОВЕТ: Если у вас планшет Apple, выберите iPhone.
- Нажмите на кнопку **Next**.
- **Используйте следующие рекомендации по загрузке приложения Google Authenticator на устройство Android (Google Play) или устройство Apple (App Store).**
- На смартфоне или планшете перейдите в Google Play (устройство Android) или в App Store (устройство Apple). Убедитесь, что на вашем смартфоне или планшете установлена последняя версия операционной системы (ОС).
- В Google Play (устройство Android) или App Store (устройство Apple) найдите приложение Google Authenticator.
- Выберите приложение Google Authenticator.
- Скачайте и установите приложение.
- После установки приложения Google Authenticator на смартфон или планшет найдите приложение на своем устройстве и откройте его. *(ПРИМЕЧАНИЕ: Внешний вид приложения может немного отличаться в зависимости от версии телефона)*
- **Для работы с приложением Google Authenticator на смартфоне или планшете воспользуйтесь следующими инструкциями.**
- После выбора устройства Apple или Android на экране компьютера появится диалоговое окно с QR-кодом. QR-код появится в виде квадрата, заполненного черными точками.

  - Если вы не можете отсканировать QR-код смартфоном или планшетом, нажмите на опцию **Can't Scan?** под QR-кодом на экране вашего компьютера.

- Если вы можете отсканировать QR-код смартфоном или планшетом, найдите приложение Google Authenticator и откройте его, если оно еще не открыто.
- Нажмите кнопку **Get Started** («Начать»).
- Вам будет предоставлена возможность **Scan a QR** («Отсканировать QR-код») или **Enter a setup key** («Ввести ключ»). Выберите одно.

  СОВЕТ: Если вы не можете отсканировать код, выберите **Enter a setup key** («Ввести ключ»). Инструкции по вводу ключа см. ниже.

- Если у вас телефон Android, приложение запросит разрешение на использование вашей камеры. Нажмите While Using the App («Во время использования приложения»).
- Если у вас телефон Apple, вы увидите сообщение *«Authenticator» Would Like to Access the Camera (*«Аутентификатор» хочет получить доступ к камере). Нажмите OK.
- После получения разрешения на использование камеры на экране вашего смартфона появится пустой экран с квадратом в центре.
- Наведите камеру смартфона или планшета на QR-код, находящийся на экране компьютера так, чтобы QR-код на экране компьютера появился в зеленом поле на экране смартфона. Приложение автоматически отсканирует код в ваш телефон или планшет.
- **Если вместо сканирования QR-кода вы выбрали ввод ключа в приложении, воспользуйтесь следующими инструкциями.**
- На экране вашего компьютера появится Секретный ключ. Это код, который вы введете в приложении Google Authenticator. Появится экран, содержащий инструкции по вводу ключа.
- В приложении Google Authenticator появится окно для ввода данных учетной записи. На этом экране укажите следующие сведения:
  - Ваше имя пользователя на сайте NY.gov в поле «Account name».
  - Ваш секретный ключ в поле «Your Key».
  - Выберите «Time-Based» в раскрывающемся списке Type of Key («Тип ключа»).
- Нажмите на кнопку **Add** («Добавить»).
- **Используйте следующие инструкции, чтобы ввести код из приложения Google Authenticator в компьютер.**
- После того как приложение успешно отсканирует QR-код или вы успешно введете в приложение Секретный ключ, приложение покажет вам экран с вашим именем пользователя и шестизначным кодом. Это код, который вы

будете вводить в компьютер на следующих шагах. Этот код будет меняться каждые 30 секунд.

- Введите шестизначный код из приложения в поле Enter Code («Введите код») на мониторе компьютера и нажмите кнопку **Verify** («Подтвердить»).
- Вы будете перенаправлены обратно на экран регистрации, где можно настроить другой метод многофакторной аутентификации. Обратите внимание, что Google Authenticator теперь находится под заголовком Enrolled factors («Задействованные факторы»).

  СОВЕТ: Рекомендуется настроить более одного метода многофакторной аутентификации.
- Когда вы настроите все нужные вам методы многофакторной аутентификации, нажмите кнопку **Finish**.

  СОВЕТ: Если вы будете настраивать метод многофакторной аутентификации, использующий приложение для телефона, загрузите приложение до нажатия кнопки **Setup** на странице браузера «Set up multifactor authentication». В приложениях используются два метода многофакторной аутентификации: Okta Verify и Google Authenticator.

Возможные сообщения об ошибках и способы их устранения.

- Сообщение об ошибке: Время сессии истекло.
- Устранение проблемы: Клиент должен снова войти в систему.

- Сообщение об ошибке: Токен не совпадает.
- Устранение проблемы:
  - Клиент должен проверить верность информации.
  - Клиент должен снова отправить (нажать «Send») код.

- Сообщение об ошибке: Обнаружена ошибка.
- Устранение проблемы: Клиент должен ввести код.

- Сообщение об ошибке: Штрих-код не сканируется.
- Устранение проблемы:
  - Попробуйте использовать альтернативные методы.
    - «Отправить активацию по SMS» – Клиент может ввести номер телефона.
    - «Настроить вручную без веб-пуша» – Клиент увидит временный код.

- «Отправить письмо активации» – Клиенту будет отправлено письмо на электронный ящик, использованный при создании учетной записи.
- Убедитесь, что устройство клиента «разрешило» доступ к камере.

Вернуться на главную страницу

Настройка аутентификатора Okta Verify для многофакторной аутентификации

На экране вашего компьютера появится окно с предложением настроить многофакторную аутентификацию.

- Загрузите на свой смартфон приложение Okta Verify. Инструкции по скачиванию приложения см. ниже.
- На экране компьютера нажмите кнопку **Setup** под Okta Verify, чтобы начать процесс установки.
- Выберите iPhone или Android в зависимости от вашего устройства.
    - вам будет предложено загрузить приложение Okta Verify из Google Play Store (Android) или из App Store (iPhone). Если вы еще не сделали этого, вам следует загрузить это приложение прямо сейчас. Инструкции по скачиванию приложения см. ниже.

  СОВЕТ: Если у вас планшет Apple, выберите iPhone.
- Нажмите на кнопку **Next**.
- **Используйте следующие рекомендации по загрузке приложения Okta Verify на устройство Android (Google Play) или устройство Apple (App Store).**
- На смартфоне или планшете перейдите в Google Play (устройство Android) или в App Store (устройство Apple). Убедитесь, что на вашем смартфоне или планшете установлена последняя версия операционной системы (ОС).
- BGoogle Play или App Store найдите приложение Okta Verify.
- Выберите мобильное приложение Okta Verify.
- Скачайте и установите приложение.
- После установки приложения Okta Verify на смартфон или планшет найдите приложение на своем устройстве и откройте его.
- **Используйте следующие инструкции для установки приложения Okta Verify на смартфоне или планшете.**
- На экране вашего компьютера появится диалоговое окно с кодом QR. QR-код появится в виде квадрата, заполненного черными точками.
    - Если вы не можете отсканировать QR-код, нажмите на опцию **Can't**

Scan? под QR-кодом на экране вашего компьютера. Указания по настройке Okta Verify после нажатия кнопки Can't Scan («Не могу отсканировать») см. ниже.

- Если вы можете отсканировать QR-код, найдите приложение Okta Verify на своем устройстве и откройте его.
- Нажмите кнопку **Get Started** («Начать»).
- Нажмите **Next** («Вперед»).
- Нажмите **Add Account**. («Добавить учётную запись»).
- Нажмите **Other** («Другое»).
- Вам будет предоставлена возможность **Scan a QR** («Отсканировать QR-код») или **Enter Key Manually** («Ввести ключ вручную»). Выберите одно.
    - Чтобы **Ввести ключ вручную**, необходимо выполнить действия, описанные ниже в разделе «Can't Scan» для подтверждения вручную без Push-уведомления.
- **Далее приведены инструкции по использованию приложения Okta Verify для сканирования QR-кода.**
- Если у вас устройство Android, приложение запросит разрешение на использование вашей камеры. Нажмите OK.
- Если у вас устройство Apple, вы увидите сообщение *«Okta Verify» Would Like to Access the Camera (*«Okta Verify» хочет получить доступ к камере). Нажмите OK.
- Наведите камеру смартфона или планшета на QR-код, находящийся на экране вашего компьютера. Приложение автоматически отсканирует код в ваш телефон или планшет.
- На мониторе вашего компьютера появится экран регистрации и всплывающее окно с QR-кодом.
- В приложении Okta Verify нажмите **Add Account** («Добавить учетную запись»).
- Наведите камеру смартфона или планшета на QR-код на экране вашего компьютера.
- После сканирования QR-кода в приложении появится новый экран с вопросом Allow Push Notifications? («Разрешить Push-уведомления?»). Выберите **Allow** («Разрешить») или **Skip** («Пропустить»).
- После успешного сканирования QR-кода в смартфон на экране вашего компьютера появится сообщение об успешном сканировании кода.
- **Используйте следующие инструкции для установки приложения Okta Verify по электронной почте или SMS после нажатия на кнопку Can't Scan.**
- После нажатия на кнопку **Can't Scan** на экране компьютера появится окно с надписью Setup Okta Verify («Настройка Okta Verify»). На этом экране

выпадающий список, в котором предлагаются следующие варианты: Send activation link via email («Отправить ссылку активации по электронной почте»), Send activation link via SMS («Отправить ссылку активации по SMS») и Setup Manually Without Push Notification («Настроить вручную без Push-уведомления»).

СОВЕТ: Ниже приведены инструкции по настройке вручную без Push-уведомлений.

- Нажмите на **Send activation link via email** («Отправить ссылку активации по электронной почте») или **Send activation link via SMS** («Отправить ссылку активации по SMS»). Вам будет отправлена ссылка.

СОВЕТ: Вы **должны** нажать на ссылку со своего смартфона или планшета.

- На смартфоне или планшете перейдите в приложение электронной почты или текстовых сообщений, чтобы получить доступ к ссылке. Откройте отправленное вам электронное или текстовое сообщение. Нажмите на ссылку, содержащуюся в сообщении.
- Ссылка приведет вас на веб-сайт Okta Verify.
- Нажмите кнопку **Get Started** («Начать»).
- Ваш смартфон подключится к веб-сайту Okta Verify и верифицирует ссылку. На экране вашего компьютера появится сообщение об успешном сканировании кода.
- **Используйте следующие инструкции для установки приложения Okta Verify с помощью функции «Вручную без Push-уведомления» из выпадающего списка «Can't Scan».**
- После нажатия на кнопку **Can't Scan** на экране компьютера появится окно с надписью Setup Okta Verify («Настройка Okta Verify»). На этом экране выпадающий список, в котором предлагаются следующие варианты: Send activation link via email («Отправить ссылку активации по электронной почте»), Send activation link via SMS («Отправить ссылку активации по SMS») и Setup Manually Without Push Notification («Настроить вручную без Push-уведомления»).
- Выберите вариант: Подтвердить вручную без Push-уведомления.
- Вы попадете на экран, сообщающий секретный ключ.
- Откройте приложение Okta Verify.
- Нажмите кнопку **Get Started** («Начать»).
- Нажмите **Next** («Вперед»).
- Нажмите **Add Account**. («Добавить учётную запись»).
- Нажмите **Other** («Другое»).
- Выберите **Enter Key Manually** («Ввести ключ вручную»).
- Введите код с экрана компьютера на экран смартфона. На смартфоне вы

введете Имя учетной записи (созданное вами) и секретный ключ, указанный на мониторе вашего компьютера.

- Нажмите **Add Account**. («Добавить учётную запись»).
    - После верификации вашего кода на экране вашего компьютера появится сообщение об успешном сканировании кода.
- Нажмите на **Done**.
- **Используйте следующие инструкции после успешного сканирования QR-кода или верификации кода вручную с помощью приложения.**
- После сканирования QR-кода приложение перейдет на экран с шестизначным кодом. Этот код будет меняться каждые 30 секунд.

- После успешной установки приложения Okta Verify на экране вашего компьютера появится экран Enroll, где вы сможете настроить другой метод многофакторной аутентификации. Теперь на экране будет показано, что Okta Verify находится под заголовком Enrolled factors («Задействованные факторы»).
- Когда вы настроите все нужные вам методы многофакторной аутентификации, нажмите кнопку «Finish».

    СОВЕТ: Если вы будете настраивать метод многофакторной аутентификации, использующий приложение для телефона, загрузите приложение до нажатия кнопки **Setup** на странице браузера «Set up multifactor authentication». В приложениях используются два метода многофакторной аутентификации: Okta Verify и Google Authenticator.

Возможные сообщения об ошибках и способы их устранения.

- Сообщение об ошибке: Время сессии истекло.
- Устранение проблемы: Клиент должен снова войти в систему.

- Сообщение об ошибке: Токен не совпадает.
- Устранение проблемы:
    - Клиент должен проверить верность информации.
    - Клиент должен снова отправить (нажать «Send») код.

- Сообщение об ошибке: Обнаружена ошибка.
- Устранение проблемы: Клиент должен ввести код.

- Сообщение об ошибке: Штрих-код не сканируется.
- Устранение проблемы:

- Попробуйте использовать альтернативные методы.
  - «Отправить активацию по SMS» – Клиент может ввести номер телефона.
  - «Настроить вручную без веб-пуша» – Клиент увидит временный код.
  - «Отправить письмо активации» – Клиенту будет отправлено письмо на электронный ящик, использованный при создании учетной записи.
- Убедитесь, что устройство клиента «разрешило» доступ к камере.

Вернуться на главную страницу

Подтверждение по SMS

На экране вашего компьютера должно появиться окно с предложением настроить многофакторную аутентификацию.

- Нажмите кнопку Setup под SMS Authentication.
- Вам будет предложено ввести номер телефона.

  СОВЕТ: Ваш номер телефона должен поддерживать прием текстовых сообщений.
- После ввода номера телефона нажмите **Send code** («Отправить код»).
- Вы получите текстовое сообщение с кодом. Введите этот код в поле Enter Code.
- Нажмите **Verify** («Подтвердить»).
- Вы будете перенаправлены на экран регистрации многофакторной аутентификации. Обратите внимание, что SMS Authentication теперь находится под заголовком Enrolled factors («Задействованные факторы»).
- Рекомендуется настроить более одного метода многофакторной аутентификации.
- Когда вы настроите все нужные вам методы многофакторной аутентификации, нажмите кнопку **Finish**.

Вернуться на главную страницу

Аутентификация через голосовой звонок

На экране вашего компьютера должно появиться окно с предложением настроить многофакторную аутентификацию.

- Нажмите кнопку Setup под Voice Call Authentication («Голосовая аутентификация»).
- Вам будет предложено ввести номер телефона.

- После ввода номера телефона нажмите **Call** («Позвонить»).
- Вам позвонят по телефону. Когда вы ответите на звонок, записанный голос зачитает вам пятизначный номер.

  СОВЕТ: Номер будет зачитан только один раз. Обязательно подготовьте бумагу и ручку, чтобы записать номер.
- Введите этот код в поле Enter Code.
- Нажмите **Verify** («Подтвердить»).
- Вы будете перенаправлены на экран регистрации многофакторной аутентификации. Обратите внимание, что Голосовая аутентификация (Voice Call Authentication) теперь находится под заголовком Enrolled factors («Задействованные факторы»).
- Рекомендуется настроить более одного метода многофакторной аутентификации.
- Когда вы настроите все нужные вам методы многофакторной аутентификации, нажмите кнопку «Finish».

Вернуться на главную страницу